WHAT IS CLAIMED IS:

1. A server device comprising:

a processor for issuing and guaranteeing public key certification;

a memory for holding information on prefix allocation allow/prohibit information of a terminal device; and

a communications interface for receiving a public key issue certification request from said terminal device and rewriting said prefix allocation allow/prohibit information, and

said processor structured to run a routine wherein public key certification issue request is received from said terminal device, a public key certification of said terminal device is issued by the server device; said prefix allocation allow/prohibit information is rewritten by the server device, and said certification is sent to said terminal device from the server device.

2. A server device according to claim 1, further comprising:

said processor structured to run a routine wherein the communications interface communicates with an information processing device containing a prefix allocation section, and

wherein an inquiry on whether prefix allocation is allowed or prohibited is received from said information processing device, said information terminal device prefix allocation allow/prohibit information is searched, and allow/prohibit information acquired is sent to said information processing device from said server device to authorize or deny the prefix allocation.

3. A server device according to claim 1, wherein the communications interface communicates with a terminal control device for managing the terminal device and for managing location information of the terminal device,

said processor is structured to run a routine

wherein an inquiry on whether prefix allocation is allowed or prohibited is received from said terminal control device, said prefix allocation allow/prohibit information is searched by the server, and the information acquired is sent to said terminal control device from the server device.

4. A terminal control device comprising:

a connection for communication with a server device containing a function to issue and guarantee public key certification, and prefix allocation allow/prohibit information;

a transceiver for acquiring public key certification from said server device; and

a routine to maintain security by utilizing IPsec technology, and a storage to store a terminal device location information,

wherein information confirming the identity of said terminal is received from said terminal device, and a terminal device public key certification is acquired.

5. A terminal control device according to claim 4,further comprising:

an information processing device having a prefix allocation function;

wherein information confirming the identity of said terminal is received from said terminal device,

an inquiry for prefix information is made to said information processor device, and

a reply to the inquiry that indicative of that said prefix was allocated is made from said information processor device,

then a signal reply to the information confirming said identity of the terminal is sent to said terminal device from the transceiver.

6. A terminal control device according to claim 4, wherein a location registration request or binding update request is received from said terminal device,

and security information of said terminal device is loaded, and if said request matches said security information, then location registration or binding update of said terminal device is performed in the terminal control device.

7. A terminal control device according to claim 4,

wherein information allowing prefix allocation for said terminal device is loaded from said server device, and if said server device approves allocation of a prefix to said terminal device, then the prefix information is reported to said terminal device.

8. A terminal authentication method for a communication system containing an information processor device with a prefix allocation function, and a server device containing a processor and memory to guarantee and issue public key certification, and a visited network and a terminal device capable of connecting to said visited network, and a home network which is associated with the terminal device, and which is mutually connected with said visited network, and

a terminal control device connected to said home network via said visited network, wherein

said server device issues a public key certification to said terminal device and rewrites prefix allocation information for said terminal device;

said information processor device receives a prefix allocation request from said terminal device, and makes an inquiry for prefix allocation allow/prohibit information to said server device, and allocates prefix information to said terminal device when allocation of the prefix is approved;

said terminal control device receives information confirming the identity of the terminal device from said terminal device, and sends prefix information of said terminal device to said information processor device; and

said information processor device establishes a security association between the terminal device to which said prefix information is issued and said terminal control device.

9. A terminal authentication method according to claim 8, wherein a communication device mutually connected to a home network and a visited network sends a prefix allocation request to said information processor device.

10. A terminal authentication method according to claim 9, wherein said terminal control device receives a location registration request from said terminal device, loads said security association, and approves location registration of said terminal device when said location registration request fulfills said security association.

11. A terminal authentication method according to claim 8, wherein

said terminal control device is comprised of communication interface for communicating with said server device, and storage device for storing public key certification information for a terminal device; and

said information processor device sends prefix information to a terminal device approved by said server device.

12. A combination method for authentication and location registration of a terminal located in a visited network comprising:

powering on a terminal;

sending a router advertisement to the terminal from a visited network router;

creating a care of address (CoA) in the terminal;

sending a device authentication request to the visited network router from the terminal;

sending a public key certification issue request with a public key of the terminal and a terminal ID to a calling authority server (CA) over an IP protocol network;

issuing a public key certification issue response from the calling authority server (CA) compatible with IPv6 protocol;

sending a DHCP solicit message from the terminal to a home agent server (HA) compatible with IPv6 protocol wherein the home agent server (HA) is linked to the calling authority server and checks with the calling authority server (CA) to allow prefix allocation;

responding to the terminal with a DHCP advertise message included in an IPv6 protocol payload;

sending a DHCP request to the home agent server from the terminal;

sending a DHCP reply to the terminal with prefix delegation;

creating a home address in the terminal;

sending a home agent address discover request to the home agent server;

responding with a home agent address discovery reply from the home agent server to the terminal;

aquiring the home agent server home address in the in terminal;

establishing a IPsec security association (SA), and digital signature via IKE (internet key exchange) and a secure communication channel using phase I and II IPsec ISAKMP protocols between the terminal and a home agent server which is linked to the calling authority server (CA) and which located in a home area;

making a location binding update in the terminal using the IPsec security association (SA);

thereby providing an authentication method for verifying a terminal authenticity by linking a digital signature method with a location binding update method.

13. The method of claim 12:

wherein the terminal is an IPv6 compatible terminal with a DHCP requesting function.

14. The method of claim 12 wherein:

a device authentication server is included in the IP network for controlling ID information required to access the home agent router;

a communication gateway is included in the IP network comprising a DHCP-PD requesting router function which handles the DHCP communications to the terminal from the home agent server and the calling authority server (CA);

wherein the terminal does not have to have a DHCP function and so that terminals without DHCP functions can be authenticated and their location can be updated according to the method.

15. The method of claim 12:

wherein a HMIPv6 Mobile Anchor Point (MAP) function is included in the method in a communication device having a HMIPv6 processor and wherein the terminal is compatible with HMIPv6;

wherein the HMIPv6 processor contains a binding cache management table for holding information linking a regional care of address (RCoA) and a local care of address (LCoa);

and wherein instead of the terminal sending the sending a DHCP request instead the HMIPv6 Mobile Anchor Point (MAP) function is included in the method in a

communication device performs DCHP communications so that the terminal does not have to be a DHCP compatible terminal.

16. A combination method for authentication and location registration of a terminal located in a visited network comprising:

powering on a terminal;

sending a router advertisement to the terminal from a visited network router;

creating a care of address (CoA) in the terminal;

sending a device authentication request to the visited network router;

sending a public key certification issue request with a public key and a terminal ID to a calling authority server over an IP protocol network;

issuing a public key certification issue response from the calling authority server (CA) compatible with IPv6 protocol;

establishing a IPsec security association (SA), and digital signature via IKE (internet key exchange) and a secure communication channel using phase I and II IPsec ISAKMP protocols between the terminal in the visited network and a home agent server which is

linked to the calling authority server (CA) and which located in a home area;

making a location binding update in the terminal using the IPsec security association (SA);

sending a request to check the public key certification to the calling authority server (CA) from the home agent server;

responding from the calling authority server whether prefix allocation is allowed with a prefix and creating a home address for the terminal;

discovering and obtaining a home address of the home agent server by the terminal;

making a location binding update by the terminal using a binding cache from the home agent server;

thereby providing an authentication method for verifying a terminal authenticity by linking a digital signature method with a location binding update method.